FORTINET
High Performance Network Security

FortiOS™ Handbook - Parallel Path Processing (Life of a Packet)

VERSION 5.4.4

FORTIOS 5.4 VERSION

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

FORTICAST

http://forticast.fortinet.com

CLI REFERENCE

http://cli.fortinet.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

April 12, 2017

FortiOS™ Handbook - Parallel Path Processing (Life of a Packet)

TABLE OF CONTENTS

Change Log

Date	Change Description
April 12, 2017	Clarification to Comparison of inspection types on page 23.
March 7, 2017	Removed confusing references to sampling packets since flow based inspection inspects all packets.
June 9, 2016	Name changed from Optimal Path Processing to Parallel Path Processing.
June 8, 2016	FortiHeartBeat renamed FortiTelemetry.
April 12, 2016	More information about CP8 and CP9 processors added. Minor edits throughout.
April 11, 2016	Added more information about application control and CASI processing, NTurbo, IPSA, CP8, CP9, and NP6 processors. Edits and information added throughout the document. All flow diagrams edited.
February 22, 2016	Improvements to the flow-based content throughout the document to enhance the explanation of single-pass flow-based inspection.
December 28, 2015	Fixed some typos and other errors.
December 16, 2015	Initial FortiOS 5.4 publication.

Introduction

Directed by security policies, a FortiGate unit screens network traffic from the IP layer up through the application layer of the TCP/IP stack. The steps involved in this inspection depend on the FortiGate hardware configuration (the presence or absence of network processors such as the NP6 and content processors such as the CP8 and CP9) and on the Unified Threat Management (UTM)/Next Generation Firewall (NGFW) inspection mode (flow-based or proxy-based) of the FortiGate or VDOM.

Work on this Parallel Path Processing (formerly Life of a Packet) chapter is still in progress. It will be expanded to include updates of the examples in the 5.2 version of this document plus new examples. Also the flow diagrams will most likely change over time as we refine our approach.

This chapter describes what happens to a packet as it travels through a FortiGate unit running FortiOS 5.4.

The FortiGate unit performs three types of security inspection:

- Kernel-based stateful inspection, that provides individual packet-based security within a basic session state
- Flow-based inspection, that takes a snapshot of content packets and uses pattern matching to identify security threats in the content
- Proxy-based inspection, that reconstructs content passing through the FortiGate unit and inspects the content for security threats.

Each inspection component plays a role in the processing of a packet as it traverses the FortiGate unit en route to its destination.

How this guide is organized

This FortiOS Handbook chapter contains the following sections:

Parallel Path Processing introduces the concept of Parallel Path Processing.

Packet flow ingress and egress: FortiGates without network processor offloading describes the overall packet flow through a FortiGate with no network offloading (NP) hardware.

Packet flow: FortiGates with NP6 processors first packet of a new session similar to the previous section, the first packet in a new session that can be offloaded is processed in much the same way as on a FortiGate with no network processors.

Packet flow: FortiGates with NP6 processors - packets in an offloaded session describes the much simpler packet flow for a packet from an offloaded session.

UTM/NGFW packet flow: flow-based inspection describes how single pass UTM/NGFW processing occurs in a flow-based FortiGate or VDOM.

UTM/NGFW packet flow: proxy-based inspection describes how UTM/NGFW processing occurs in a proxy-based FortiGate or VDOM.

Comparison of inspection types shows how different security functions map to different inspection types.

Parallel Path Processing

Parallel Path Processing (PPP) uses the firewall policy configuration to choose from a group of parallel options to determine the optimal path for processing a packet. Most FortiOS features are applied through Firewall policies and the features applied determine the path a packet takes. Using firewall policies you can impose UTM/NGFW processing on content traffic that may contain security threats (such as HTTP, email and so on). Many UTM/NGFW processes are offloaded and accelerated by CP8 or CP9 processors. Using the policy configuration you can apply a range of protection from basic IPS attack protection that looks for network-based attacks to full scale advanced threat management (ATM), application control, antivirus, DLP and so on.

You can also create policies for traffic that does not pose security threats and bypass UTM/NGFW checking. This control allows you to improve network performance without compromising security. On FortiGates with network processors (for example the NP6) much of the traffic that does not require UTM/NGFW processing can be offloaded to the NP6 processors freeing up FortiGate processing resources for other higher risk traffic.

In addition, many FortiGate models support NTurbo to offload flow-based UTM/NGFW sessions to network processors. Flow-based sessions can also be accelerated using IPSA technology to enhance offloading of pattern matching to CP8 and CP9 content processors.

This chapter begins with an overview of packet flow ingress and egress and includes a section that shows how NP6 offloading optimizes packet flow for packets that don't require UTM/NGFW processing and for packets that use NTurbo to offload flow-based UTM/NGFW processing.

Next this chapter breaks down how packets pass through UTM/NGFW processing both for a single-pass flow-based UTM/NGFW processing and a proxy-based UTM/NGFW processing.

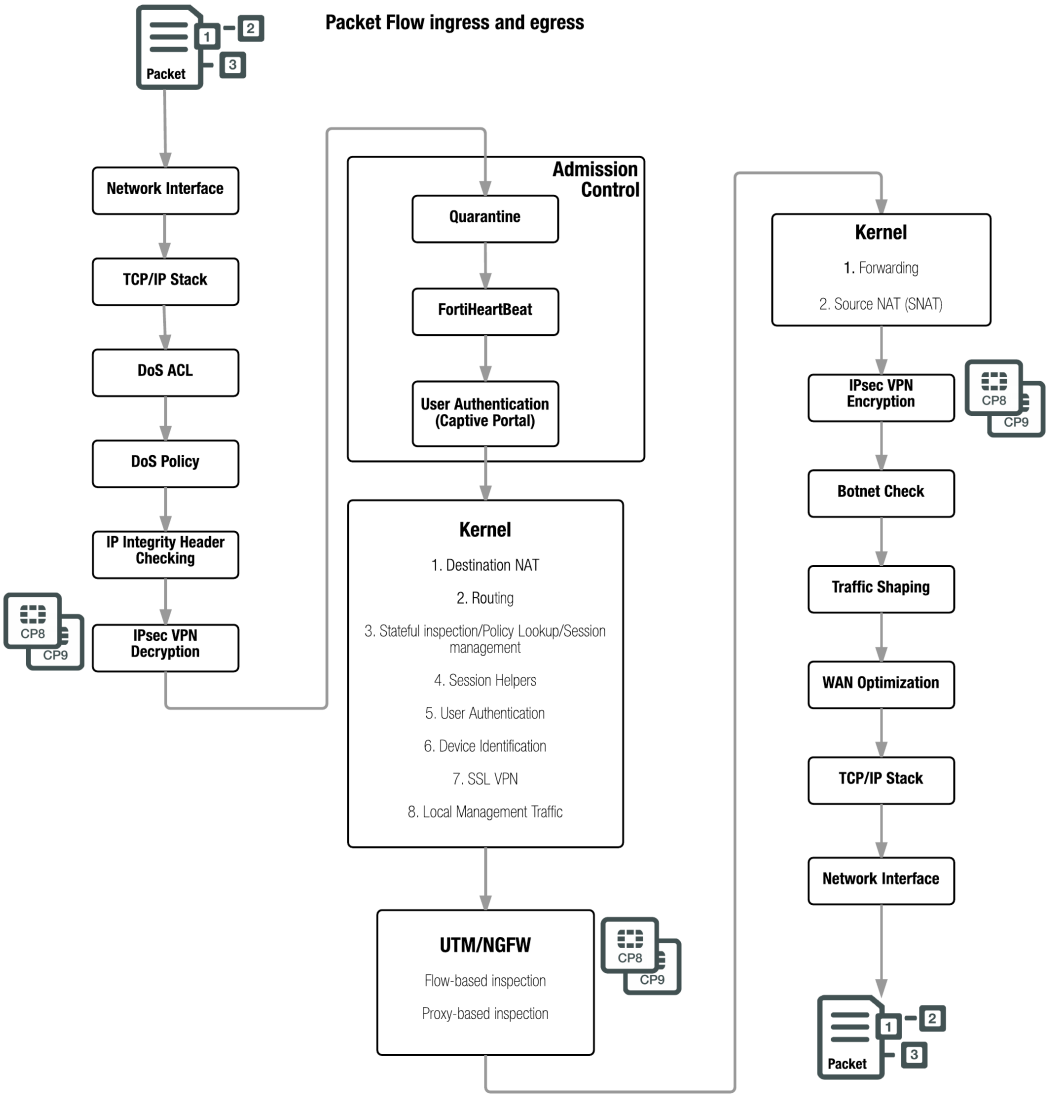
High-level list of processes that affect packets

In general packets passing through a FortiGate unit can be affected by the following processes. This is a complete high-level list of all of the processes. Not all packets see all of these processes. The processes a packet encounters depends on the type of packet and on the FortiGate software and hardware configuration.

- **Ingress packet flow**
  - Network Interface
  - TCP/IP stack
  - DoS ACL
  - DoS Policy
  - IP integrity header checking
  - IPsec VPN decryption
- **Admission Control**
  - Quarantine
  - FortiTelemetry
  - User Authentication
- **Kernel**
  - Destination NAT
  - Routing
  - Stateful inspection/Policy Lookup/Session management
  - Session Helpers
  - User Authentication
  - Device Identification
  - SSL VPN
  - Local Management Traffic
- **UTM/NGFW**
  - Flow-based inspection
    - NTurbo
    - IPSA
  - Proxy-based inspection
- **Kernel**
  - Forwarding
  - Source NAT (SNAT)
- **Egress packet flow**
  - IPsec VPN Encryption
  - Botnet check
  - Traffic shaping
  - WAN Optimization
  - TCP/IP stack
  - Network Interface

Packet flow ingress and egress: FortiGates without network processor offloading

This section describes the steps a packet goes through as it enters, passes through and exits from a FortiGate unit. This scenario shows all of the steps a packet goes through if a FortiGate does not contain network processors (such as the NP6).



Ingress

All packets accepted by a FortiGate pass through a network interface and are processed by the TCP/IP stack. Then if **DoS policies** or **Access Control List (ACL) policies** have been configured the packet must pass through these as well as automatic **IP integrity header checking**.

DoS scans are handled very early in the life of the packet to determine whether the traffic is valid or is part of a DoS attack. The DoS module inspects all traffic flows but only tracks packets that can be used for DoS attacks (for example, TCP SYN packets), to ensure they are within the permitted parameters. Suspected DoS attacks are blocked, other packets are allowed.

IP integrity header checking reads the packet headers to verify if the packet is a valid TCP, UDP, ICMP, SCTP or GRE packet. The only verification that is done at this step to ensure that the protocol header is the correct length. If it is, the packet is allowed to carry on to the next step. If not, the packet is dropped.

Incoming **IPsec packets** that match configured IPsec tunnels on the FortiGate are decrypted after header checking is done.

If the packet is an IPsec packet, the IPsec engine attempts to decrypt it. If the IPsec engine can apply the correct encryption keys and decrypt the packet, the unencrypted packet is sent to the next step. Non-IPsec traffic and IPsec traffic that cannot be decrypted passes on to the next step without being affected. IPSec VPN decryption is offloaded to and accelerated by CP8 or CP9 processors.

Admission Control

Admission control checks to make sure the packet is not from a source or headed to a destination on the quarantine list. If configured admission control then imposes FortiTelemetry protection that requires a device to have FortiClient installed before allowing packets from it. Admission control can also impose captive portal authentication on ingress traffic.

Kernel

Once a packet makes it through all of the ingress steps, the FortiOS kernel performs the following checks to determine what happens to the packet next.

Destination NAT

Destination NAT checks the NAT table and determines if the destination IP address for incoming traffic must be changed using DNAT. DNAT is typically applied to traffic from the Internet that is going to be directed to a server on a network behind the FortiGate. DNAT means the actual address of the internal network is hidden from the Internet. This step determines whether a route to the destination address actually exists. DNAT must take place before routing so that the FortiGate unit can route packets to the correct destination.

Routing

Routing uses the routing table to determine the interface to be used by the packet as it leaves the FortiGate unit. Routing also distinguishes between local traffic and forwarded traffic. Firewall policies are matched with packets depending on the source and destination interface used by the packet. The source interface is known when the packet is received and the destination interface is determined by routing.

Stateful inspection/Policy lookup/Session management

Stateful inspection looks at the first packet of a session and looks in the policy table to make a security decision about the entire session. Stateful inspection looks at packet TCP SYN and FIN flags to identity the start and end of a session, the source/destination IP, source/destination port and protocol. Other checks are also performed on the packet payload and sequence numbers to verify it as a valid session and that the data is not corrupted or poorly formed.

When the first packet is a session is matched in the policy table, stateful inspection adds information about the session to its session table. So when subsequent packets are received for the same session, stateful inspection can determine how to handle them by looking them up in the session table (which is more efficient than looking them up in the policy table).

Stateful inspection makes the decision to drop or allow a session and apply security features to it based on what is found in the first packet of the session. Then all subsequent packets in the same session are processed in the same way.

When the final packet in the session is processed, the session is removed from the session table. Stateful inspection also has a session idle timeout that removes sessions from the session table that have been idle for the length of the timeout.

See the Stateful Firewall Wikipedia article (https://en.wikipedia.org/wiki/Stateful_firewall) for an excellent description of stateful inspection.

Session helpers

Some protocols include information in the packet body (or payload) that must be analyzed to successfully process sessions for this protocol. For example, the SIP VoIP protocol uses TCP control packets with a standard destination port to set up SIP calls. To successfully process SIP VoIP calls, FortiOS must be able to extract information from the body of the SIP packet and use this information to allow the voice-carrying packets through the firewall.

FortiOS uses session helpers to analyze the data in the packet bodies of some protocols and adjust the firewall to allow those protocols to send packets through the firewall. FortiOS includes the following session helpers:

- PPTP
- H323
- RAS
- TNS
- TFTP
- RTSP
- FTP
- MMS
- PMAP
- SIP
- DNS-UDP
- RSH
- DCERPC
- MGCP

User authentication

User authentication added to security policies is handled by the stateful inspection, which is why Firewall authentication is based on IP address. Authentication takes place after policy lookup selects a policy that includes authentication.

Device identification

Device identification is applied if required by the matching policy.

SSL VPN

Local SSL VPN traffic is treated like special management traffic as determined by the SSL VPN destination port. Packets are decrypted and are routed to an SSL VPN interface. Policy lookup is then used to control how packets are forwarded to their destination outside the FortiGate. SSL encryption and decryption is offloaded to and accelerated by CP8 or CP9 processors.

Local management traffic

Local management traffic terminates at a FortiGate interface. This can be any FortiGate interface including dedicated management interfaces. In multiple VDOM mode local management traffic terminates at the management interface. In Transparent mode, local management traffic terminates at the management IP address.

Local management traffic includes administrative access, some routing protocol communication, central management from FortiManager, communication with the FortiGuard network and so on. Management traffic is allowed or blocked according to the Local In Policy list which lists all management protocols and their access control settings. You configure local management access indirectly by configuring administrative access and so on.

Management traffic is processed by applications such as the web server which displays the FortiOS web-based manager, the SSH server for the CLI or the FortiGuard server to handle local FortiGuard database updates or FortiGuard Web Filtering URL lookups.

Local management traffic is not involved in subsequent stateful inspection steps.

SSL VPN traffic terminates at a FortiGate interface similar to local management traffic. However, SSL VPN traffic uses a different destination port number than administrative HTTPS traffic and can thus be detected and handled differently.

UTM/NGFW

If the policy matching the packet includes security profiles, then the packet is subject to Unified Threat Management (UTM)/Next Generation Firewall (NGFW) processing. UTM/NGFW processing depends on the inspection mode of the FortiGate: Flow-based (single pass architecture) or proxy-based. Many UTM/NGFW processes are offloaded and accelerated by CP8 or CP9 processors.

Single pass flow-based UTM/NGFW inspection identifies and blocks security threats in real time as they are identified using single-pass Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats.

Proxy-based UTM/NGFW inspection can apply both flow-based and proxy-based inspection. Packets initially encounter the IPS engine, which can apply single-pass flow-based IPS, Application Control and CASI (as configured). The packets are then sent to the proxy for proxy-based inspection. Proxy-based inspection can apply VoIP inspection, DLP, AntiSpam, Web Filtering, Antivirus, and ICAP.

Content processors (CP8 and CP9)

Most FortiGate models contain FortiASIC Content Processors (CPs) that accelerate IPsec and SSL VPN encryption/decryption and key exchance and flow-based content processing pattern matching. CPs work at the system level with tasks being offloaded to them as determined by the main CPU. Capabilities of the CPs vary by model. Newer FortiGate units include CP8 and new CP9 processors.

CP9 capabilities

The CP9 content processor provides the following services:

- Flow-based inspection pattern matching acceleration with over 10Gbps throughput
- High performance VPN bulk data engine
- Key Exchange Processor that supports high performance IKE and RSA computation
- DLP fingerprint support

CP8 capabilities

The CP8 content processor provides the following services:

- Flow-based inspection pattern matching acceleration
- High performance VPN bulk data engine
- Key Exchange Processor that supports high performance IKE and RSA computation

Kernel

Traffic is now in the process of exiting the FortiGate unit. The kernel uses the routing table to forward the packet out the correct exit interface.

The kernel also checks the NAT table and determines if the source IP address for outgoing traffic must be changed using SNAT. SNAT is typically applied to traffic from an internal network heading out to the Internet. SNAT means the actual address of the internal network is hidden from the Internet.

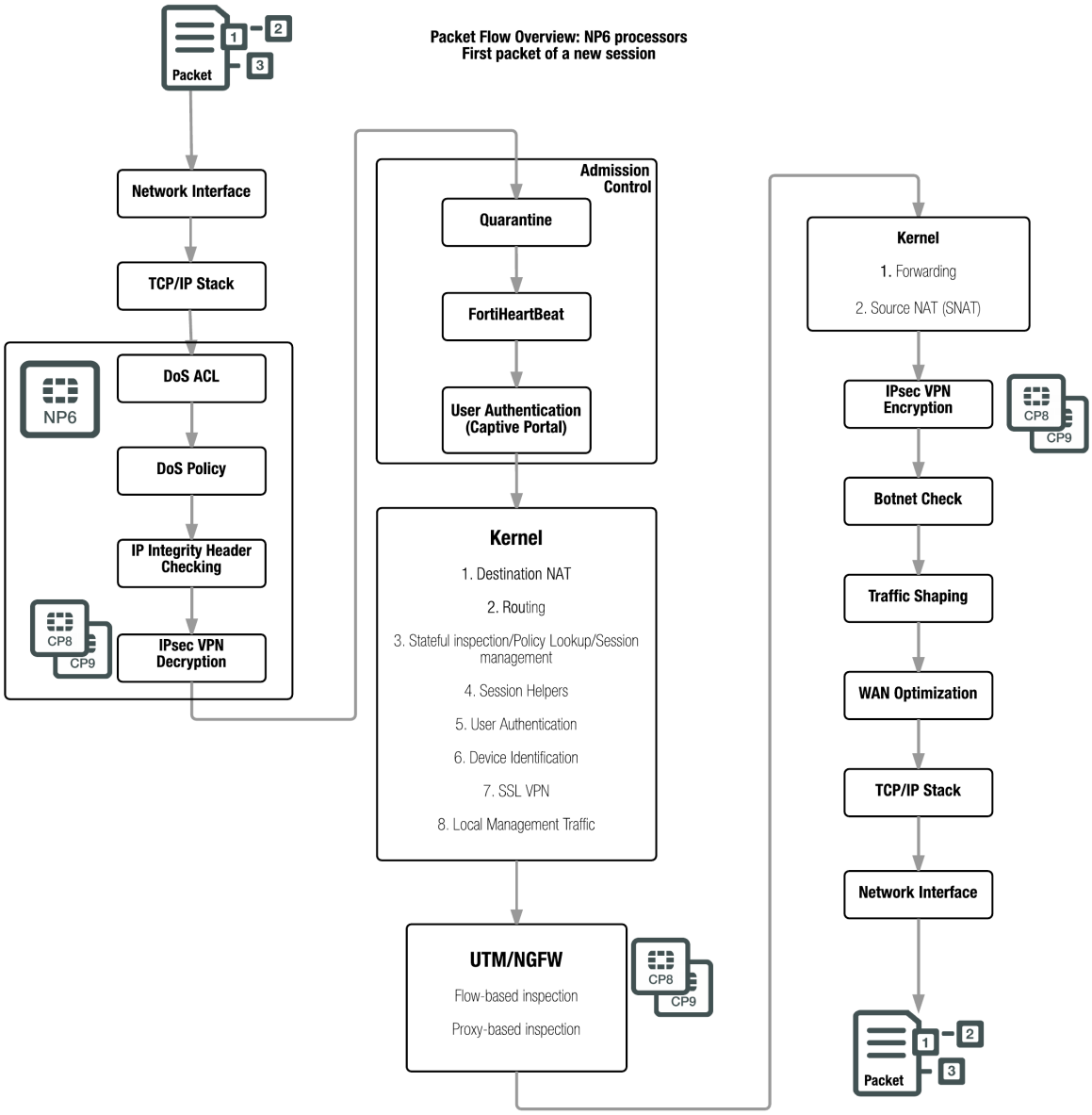
Egress

Before exiting the FortiGate outgong packets that are entering an IPsec VPN tunnel are encrypted and encapsulated. IPSec VPN encryption is offloaded to and accelerated by CP8 or CP9 processors. Packets are then subject to botnet checking to make sure they are not destined for known botnet addresses.

Traffic shaping is then imposed, if configured, followed by WAN Optimization. The packet is then processed by the TCP/IP stack and exits out the egress interface.

Packet flow: FortiGates with NP6 processors first packet of a new session

On a FortiGate with NP6 processors the first packet in a new session is handled the same way as on a FortiGate with no NP6 processors. Except that some processes, such as DoS, ACL, IP integrity checking, and IPsec VPN decryption are accelerated by the NP6 processor.



Network processors (NP6)

FortiASIC network processors work at the interface level to accelerate traffic by offloading sessions from the main CPU. Current FortiGate models contain NP6 network processors. Older FortiGate models include NP4 and older network processors.

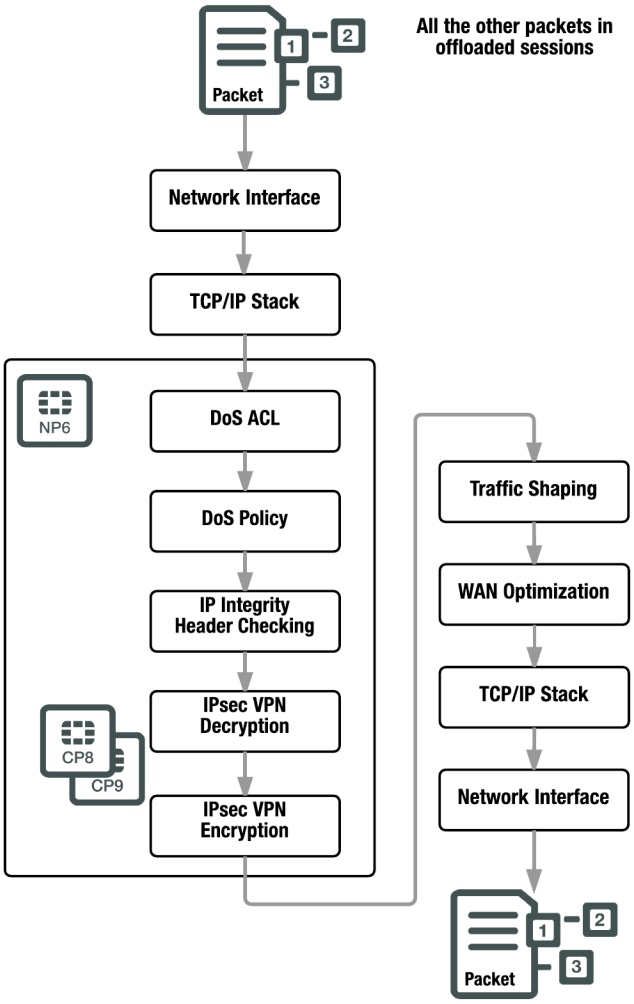
NP6 processors can offload most IPv4 and IPv6 traffic, IPsec VPN encryption, CAPWAP traffic, and multicast traffic. The NP6 has a capacity of 40 Gbps through 4 x 10 Gbps interfaces or 3 x 10 Gbps and 16 x 1 Gbps interfaces.

Sessions that require proxy-based UTM/NGFW (including proxy-based virus scanning, web filtering, and so on) are not fast pathed and must be processed by the CPU.

Sessions that require flow-based UTM/NGFW (including IPS, application control, flow-based virus scanning and so on) can be offloaded to NP4 or NP6 network processors if the FortiGate supports NTurbo.

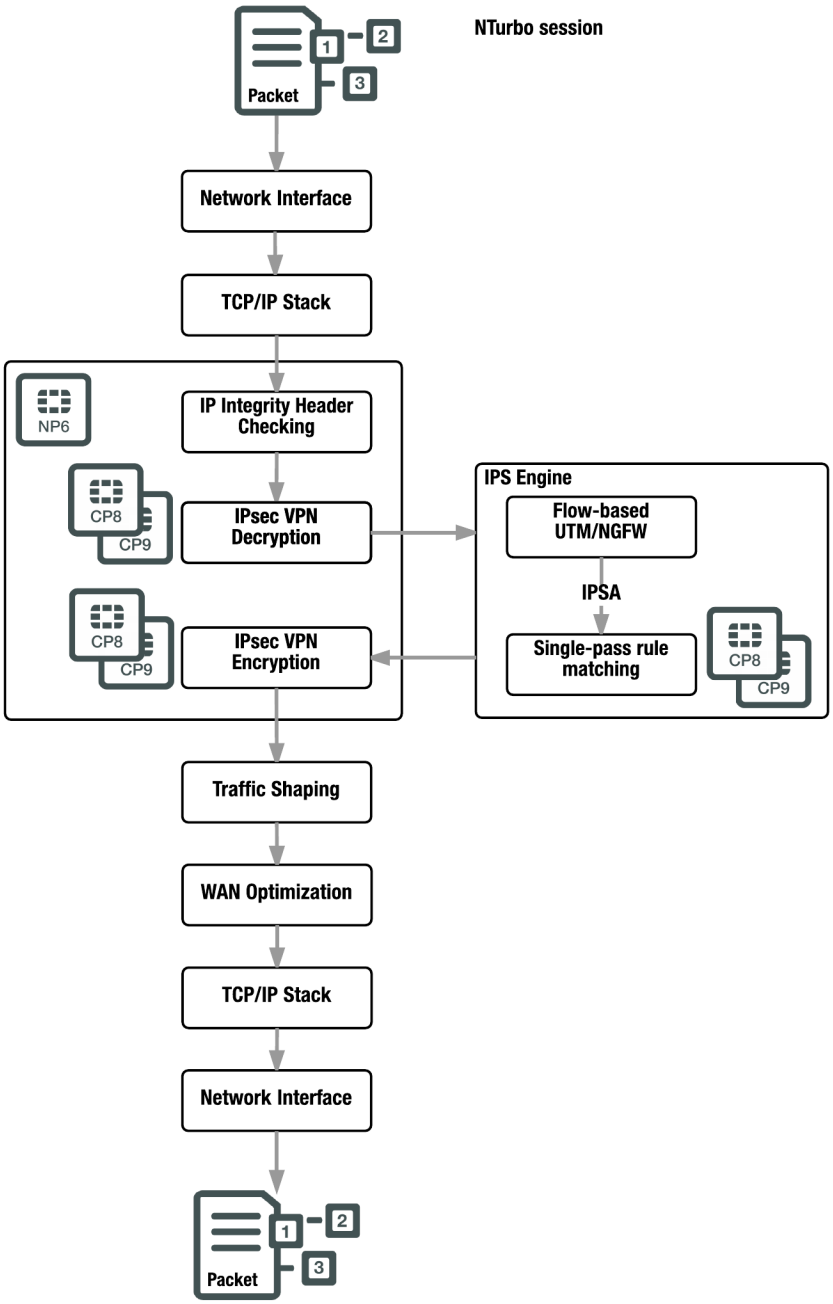
Packet flow: FortiGates with NP6 processors - packets in an offloaded session

The first packet of a session determines if the session can be offloaded. As long as there is no proxy-based UTM/NGFW, if your FortiGate includes NP6 processors, most sessions can be offloaded to them. After the first packet, subsequent packets in an offloaded session skip routing, UTM/NGFW, and kernel processors and are just forwarded out the egress interface by the NP6 processor. As well, security measures such as DoS policies, ACL, and so on are accelerated by the NP6 processor.



Packet flow: FortiGates with NP6 processors - packets in an NTurbo session

If your FortiGate supports NTurbo, many flow-based UTM/NGFW sessions can be offloaded to NP6 processors.



After the first packet, subsequent packets in an offloaded flow-based UTM/NGFW session skip routing, and kernel processors. Flow-based UTM/NGFW operations are still handled by the CPU with IPSA offloading pattern matching to CP8 or CP9 processors.

If a security threat is found the session is dropped. Otherwise, packets that are not blocked by UTM/NGFW are forwarded out of the egress interfaces by the NP6 processor.

NTurbo is not compatible with DoS polices, session helpers, or and most types of tunneling. If any of these features are present, flow-based UTM/NGFW sessions are not offloaded by NTurbo.

UTM/NGFW packet flow: flow-based inspection

Flow-based UTM/NGFW inspection identifies and blocks security threats in real time as they are identified using single-pass architecture that involves Direct Filter Approach (DFA) pattern matching to identify possible attacks or threats.

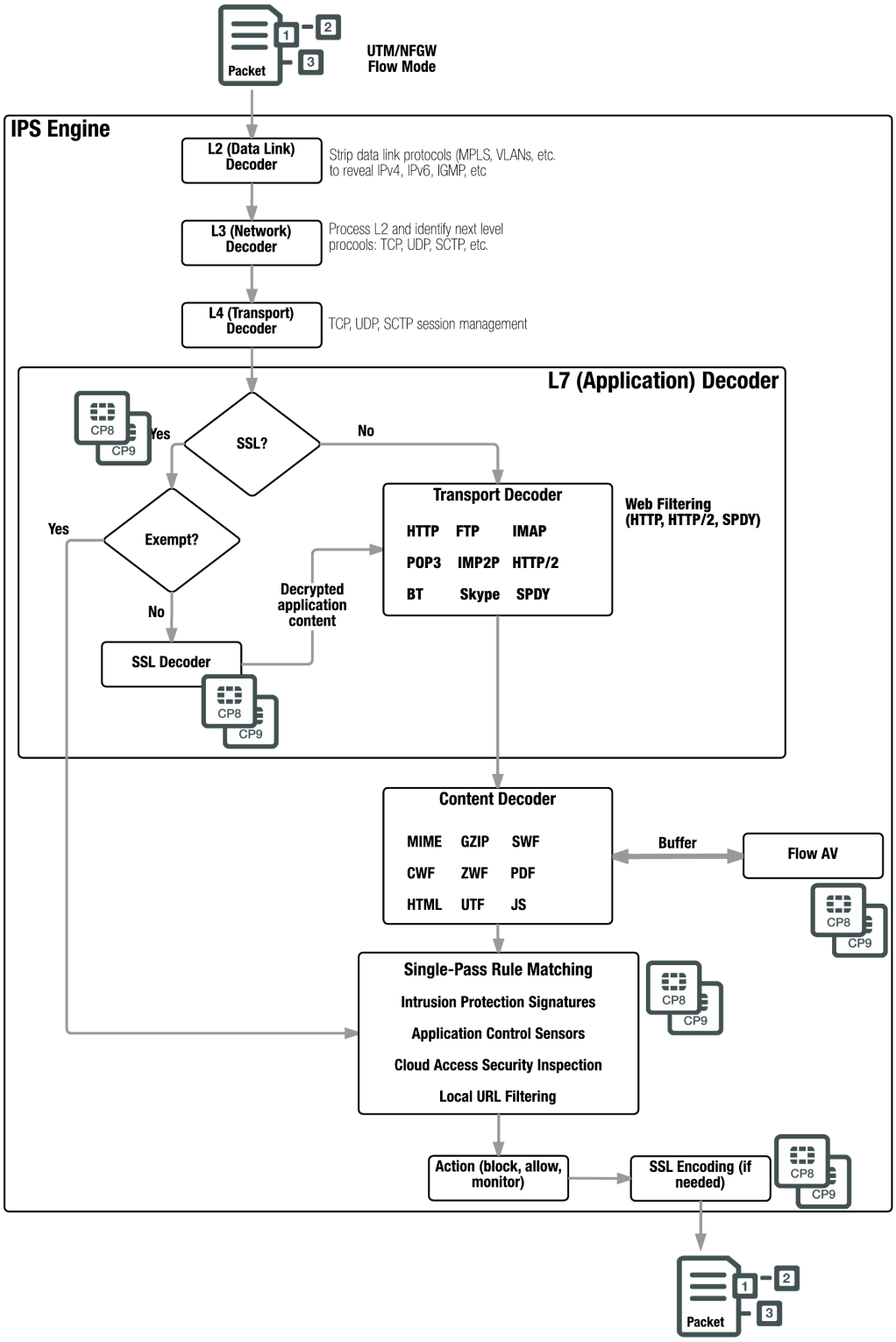
If a FortiGate or a VDOM is configured for flow-based inspection, depending on the options selected in the firewall policy that accepted the session, flow-based inspection can apply **IPS**, **Application Control**, **Cloud Access Security Inspection (CASI)**, **Web Filtering**, **DLP**, and **Antivirus**. Flow-based inspection is all done by the IPS engine and as you would expect, no proxying is involved.

Before flow-based inspection can be applied the IPS engine uses a series of decoders to determine the appropriate security modules to be applied depending on the protocol of the packet and on policy settings. In addition, if SSL inspection is configured, the IPS engine also decrypts SSL packets. SSL decryption is offloaded and accelerated by CP8 or CP9 processors

All of the applicable flow-based security modules are applied simultaneously in one single pass, and pattern matching is offloaded and accelerated by CP8 or CP9 processors. IPS, Application Control and CASI, flow-based Web Filtering and flow-based DLP filtering happen together. CASI signatures are applied as part of application control. Flow-based antivirus caches files during protocol decoding and submits cached files for virus scanning while the other matching is carried out.

Flow-based inspection typically requires less processing resources than proxy-based inspection and since its not a proxy, flow-based inspection does not change packets (unless a threat is found and packets are blocked). Flow-based inspection cannot apply as many features as proxy inspection (for example, flow-based inspection does not support client comforting and some aspects of replacement messages).

IPS, Application Control, and CASI are only applied using flow-based inspection. Web Filtering, DLP and Antivirus can also be applied using proxy-based inspection.


Packet
UTM/NFGW
Flow Mode
IPS Engine
L2 (Data Link) Decoder
Strip data link protocols (MPLS, VLANs, etc. to reveal IPv4, IPv6, IGMP, etc
L3 (Network) Decoder
Process L2 and identify next level procools: TCP, UDP, SCTP, etc.
L4 (Transport) Decoder
TCP, UDP, SCTP session management
L7 (Application) Decoder
CP8
CP9
Yes
SSL?
No
Transport Decoder
HTTP FTP IMAP
POP3 IMP2P HTTP/2
BT Skype SPDY
Web Filtering
(HTTP, HTTP/2, SPDY)
Yes
Exempt?
No
Decrypted application content
SSL Decoder
Content Decoder
MIME GZIP SWF
CWF ZWF PDF
HTML UTF JS
Buffer
Flow AV
Single-Pass Rule Matching
Intrusion Protection Signatures
Application Control Sensors
Cloud Access Security Inspection
Local URL Filtering
Action (block, allow, monitor)
SSL Encoding (if needed)
Packet

UTM/NGFW packet flow: proxy-based inspection

If a FortiGate or VDOM is configured for proxy-based inspection then a mixture of flow-based and proxy-based inspection occurs. Packets initially encounter the IPS engine, which uses the same steps described in UTM/NGFW packet flow: flow-based inspection on page 19 to apply single-pass IPS, Application Control and CASI if configured in the firewall policy accepting the traffic.

The packets are then sent to the FortiOS UTM/NGFW proxy for proxy-based inspection. The proxy first determines if the traffic is SSL traffic that should be decrypted for SSL inspection. SSL traffic to be inspected is decrypted by the proxy. SSL decryption is offloaded to and accelerated by CP8 or CP9 processors.

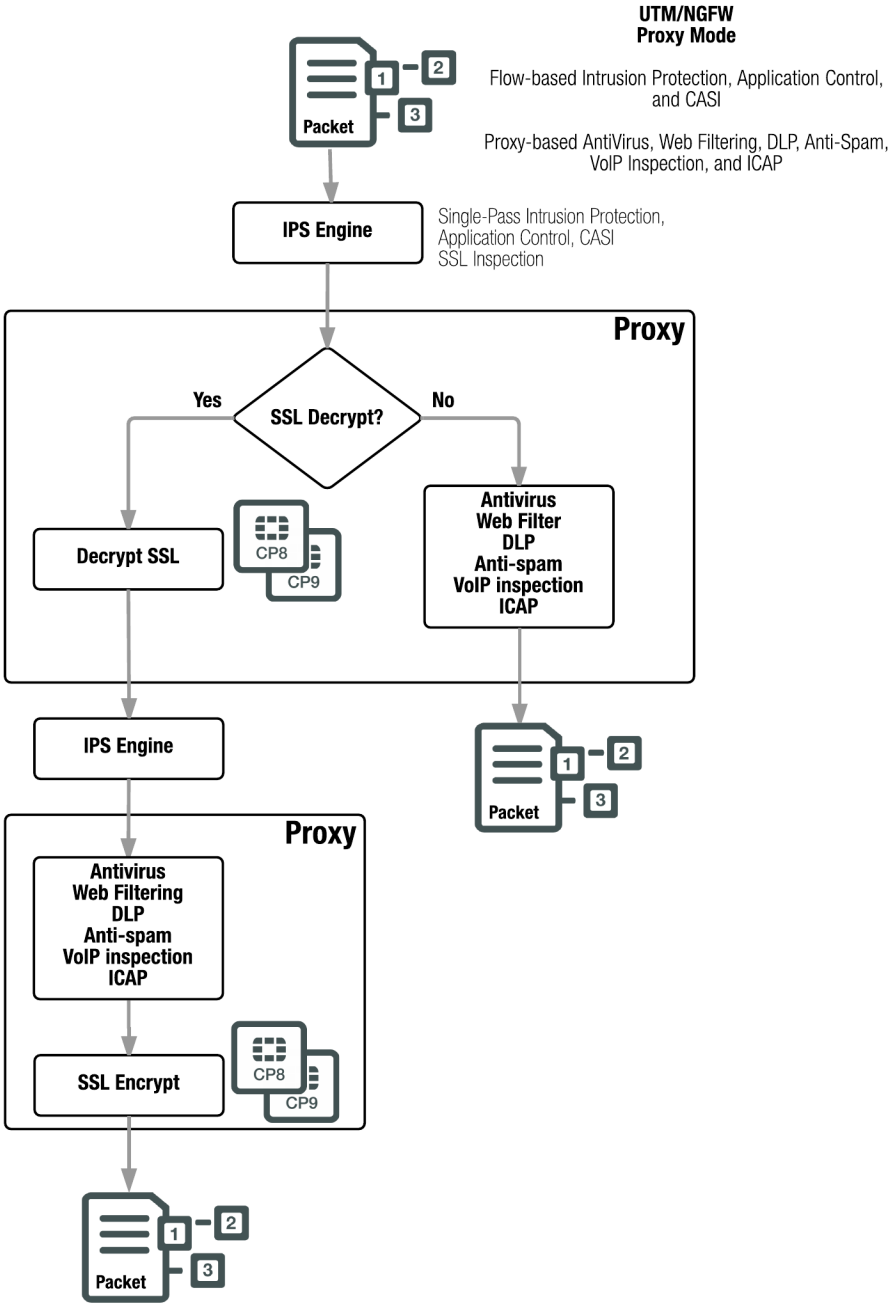
Proxy-based inspection extracts and caches content, such as files and web pages, from a content session and inspects the cached content for threats. Content inspection happens in the following order: **VoIP inspection**, **DLP**, **AntiSpam**, **Web Filtering**, **Antivirus**, and **ICAP**.

If no threat is found the proxy relays the content to its destination. If a threat is found the proxy can block the threat and replace it with a replacement message.

Decrypted SSL traffic is sent to the IPS engine (where IPS, Application Control, and CASI can be applied) before re-entering the proxy where actual proxy-based inspection is applied to the decrypted SSL traffic. Once decrypted SSL traffic has been inspected it is re-encrypted and forwarded to its destination. SSL encryption is offloaded to and accelerated by CP8 or CP9 processors. If a threat is found the proxy can block the threat and replace it with a replacement message.

The proxy can also block VoIP traffic that contains threats. VoIP inspection can also look inside VoIP packets and extract port and address information and open pinholes in the firewall to allow VoIP traffic through.

ICAP intercepts HTTP and HTTPS traffic and forwards it to an ICAP server. The FortiGate is the surrogate, or “middle-man”, and carries the ICAP responses from the ICAP server to the ICAP client; the ICAP client then responds back, and the FortiGate unit determines the action that should be taken with these ICAP responses and requests.


UTM/NGFW
Proxy Mode
Flow-based Intrusion Protection, Application Control, and CASI
Proxy-based AntiVirus, Web Filtering, DLP, Anti-Spam, VoIP Inspection, and ICAP
Packet
IPS Engine
Single-Pass Intrusion Protection, Application Control, CASI SSL Inspection
Proxy
Yes
SSL Decrypt?
No
Decrypt SSL
CP8
CP9
Antivirus
Web Filter
DLP
Anti-spam
VoIP inspection
ICAP
IPS Engine
Packet
Proxy
Antivirus
Web Filtering
DLP
Anti-spam
VoIP inspection
ICAP
SSL Encrypt
CP8
CP9
Packet

Comparison of inspection types

The tables in this section show how different security functions map to different inspection types.

Mapping security functions to inspection types

The table below lists FortiOS security functions and shows whether they are applied by the kernel, flow-based inspection or proxy-based inspection. This table does not indicate which inspection types are available depending on the inspection mode. When the inspection mode is set to proxy all inspection types are available. When the inspection mode is set to flow-based then proxy-only inspection types are not available.

FortiOS security functions and inspection types

Security Function	Kernel (Stateful inspection)	Flow-based inspection	Proxy-based inspection
Firewall	yes		
IPsec VPN	yes		
Traffic Shaping	yes		
User Authentication	yes		
Management Traffic	yes		
SSL VPN	yes		
IPS		yes	
Antivirus		yes	yes
Application Control		yes	
CASI		yes	
Web filtering		yes	yes
DLP		yes	yes
Anti-Spam			yes
VoIP inspection			yes
ICAP			yes

FORTINET®

High Performance Network Security